暗号化電子メールシステム

2R−3　館林 誠　松崎 なつめ　原田 俊治　宮地 充子　多田 信彦

松下電器産業（株）　情報通信研究センター

1．はじめに

UNIX*) ワークステーションをベースにした電子メールは、技術・学術分野で有効な通信手段の1つになってきている。そして、これに秘匿機能や認証機能を追加した暗号化電子メールもいくつか開発され発表されている[1],[2]**)。

暗号化電子メールを、さらに普及するためには、少なくとも以下の条件が必要である。

（1）暗号文フォーマットや暗号化手続きの標準的な枠組み

（2）十分な安全性と処理速度

（3）移植性、互換性や操作性などシステムとしての利便性

今回、インターネットの標準案[3]~[5]に沿った上で、上記条件を満たすべく実用的な暗号化電子メールを開発したので報告する。

2．設計方針

本システムの設計方針は以下のとおりである。

（1）インターネットの標準案PEM(Privacy Enhanced Mail)に準拠。

（2）安全で高速な暗号化アルゴリズムを開発し、使用。

（3）公開鍵ディレクトリ、ICカードを用いた鍵管理により安全性を保ちつつ利便性を向上。

（4）従来のUNIXメールシステムを包含するインプリメント

上記それぞれに対し、以降で詳細に説明する。

3．PEM準拠

代表的なネットワークの1つインターネットでは、現在電子メールの暗号化の標準化作業がDraft Standardの状態で、具体的な標準案PEMが固まりつつある[3]~[5]。

本システムは、この標準案に準拠しており、以下の特徴を備えている。

（1）ハイブリッド型暗号

暗号化には、公開鍵暗号と秘密鍵暗号を組み合わせたハイブリッド型暗号を用いる。図1に構成を示す。メッセージは、高速な秘密鍵暗号を用いて暗号化し、そこで用いるセッション鍵は、鍵管理の容易な公開鍵暗号を用いて暗号化する。また、署名はメッセージの圧縮値に対して、公開鍵署名方法を用いて生成／認証する。

（2）証明書による鍵管理

公開鍵暗号を用いる場合、相手の公開鍵として用いるデータの完全性を確保することが必要になる。本システムでは、鍵発行センターを設置し、このセンターが各ユーザの公開鍵に対して証明書を発行する。ユーザは相手の公開鍵の正当性をこの証明書で確認する。

（3）PEMに準拠した暗号文フォーマット

暗号文は暗号化されたセッション鍵や署名および送信者の証明書を格納した暗号化ヘッダ部と、暗号化されたメッセージを格納した暗号化テキスト部に構造化され、通常の電子メールのテキスト部に格納される。

4．暗号化アルゴリズム

本システムでは、公開鍵暗号として楕円曲線上のElGamal暗号を採用している。また署名には同じ楕円曲線上のElGamal署名を採用している。構成した楕円曲線暗号は[6][7]に詳細に述べている。これを採用すると公開鍵のデータ量を従来の1/5にすることができるため、同じ安全性を持つRSA暗号と比べて高速処理が実現できる。また、鍵管理の負担も軽減される。

Security Enhanced Electronic Mail System
Makoto TATEBAYASHI , Natsume MATSUZAKI ,
Shunji HARADA , Atsuko MIYAJI , Nobuhiko TADA
MATSUSHITA ELECTRIC INDUSTRIAL CO.,LTD.

*)UNIXオペレーティングシステムは、UNIXシステムラボラトリーズ社が開発し、ライセンスしています。

**)この他、富士通がASIACRYPT'91展示会で暗号化電子メールを出展

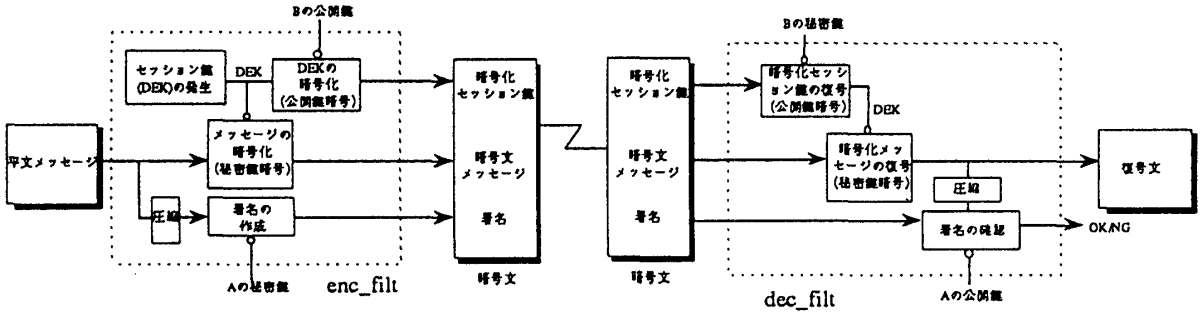

図1

5. 鍵管理

・公開鍵の管理

基本的には各ユーザが自分の公開鍵を、鍵管理センター発行の証明書とともに管理する。これに加え本システムでは、UNIXに実装されているDNS(Domain Name System)やNIS(Network Information Service)をオンラインデータベースとして用いることを可能とする。これによりユーザの公開鍵の配付や参照などが容易に行える。

・秘密鍵の管理

各ユーザが、自分のパスワードにより暗号化した秘密鍵ファイルを管理する。また、自分の秘密鍵をICカードに格納して管理することも可能である。これにより高いセキュリティで携帯性にすぐれた秘密鍵の管理を実現する。

6. インプリメント

システムの特徴

・暗号化・署名生成／復号・署名認証機能を、フィルタとして実現 (enc_filt,dec_filt)
・Emacsから用いるRmail,mh-eおよび独自のメールインタフェースに、前記フィルタをアドオン
・すべてソフトウェアで実現、移植性を向上
・ユーザに暗号化を意識させない自動暗号化／復号機能を装備。
・誤配信防止の機能を装備
・オンラインデータベースから公開鍵を自動的に取得。
・ICカードとパスワードによる秘密鍵の管理

諸特性

・処理時間：28MIPSのワークステーションで、A4 1枚のメッセージの処理時間を実測
enc_filt,dec_filt…各0.3秒（CPU時間）
Emacsから用いた場合の処理時間…1.5秒
（オンラインデータベースからの公開鍵取得時間を含む）
・ディスク容量：実行モジュール3MB
・メモリ容量： 1MB～1.5MB

7. おわりに

本稿では、インターネットの標準案を元に、処理速度の面、およびシステムとしての利便性の面で従来より実用的な暗号化電子メールの提案を行った。現在このシステムは、社内で運用、評価中である。

参考文献

【1】S.Kawamura A.Shinbo K.Takabayashi, "E-mail implementation of a one-way key distribution scheme", 第14回情報理論とその応用シンポジウム(SITA'91), 1991.

【2】岡本、小林、桜井、" 零知識証明を利用した検印付き電子メールシステム" 、情報処理学会第44回（平成4年前期）全国大会, 1992.

【3】RFC[1113F], J.Linn, "Privacy Enhancement for Internet Electronic Mail:Part I: Message Encryption and Authentication Procedures", August, 1992.

【4】RFC[1114H], S.Kent, "Privacy Enhancement for Internet Electronic Mail:Part II: Certificate-Based Key Management", August, 1992.

【5】RFC[1115D], J.Linn, "Privacy Enhancement for Internet Electronic Mail:Part III: Algorithms, Modes, and Identifiers", D.Balenson, August, 1992.

【6】A.Miyaji, "On ordinary elliptic curves", Abstract of proceedings of ASIACRYPT'91, 1991.

【7】A.Miyaji, "Elliptic curves over Fp suitable for cryptosystems", Abstract of proceedings of AUSCRYPT'92, 1992.